REMARKS

In accordance with the foregoing, claims 1-4, 6-24 and 26-41 are pending and under consideration.

CLAIM REJECTIONS UNDER 35 USC § 102

Claims 1-4, 6-24, and 26-41 are rejected under 35 U.S.C. 102(b) as allegedly being anticipated by NPL to NII (JP H10-333902). Applicant respectfully traverses the rejection in view of the following discussion of the claimed subject matter vis-à-vis to the applied prior art reference's teachings.

Independent claim 1 is directed to an information reproducing apparatus having (1) a hardware secure module having a tamper resistant module structure and storing information related to secure software, (2) a memory that stores the secure software, (2) a falsification checking unit, and (4) a processor that executes the secure software the falsification checking unit determines that the secure software is not falsified.

The falsification checking unit that is loaded on the hardware secure module reads the secure software from the memory by direct access without using an operating system, compares the secure software with the information in the hardware secure module, and determines whether the secure software is falsified based on a result of the comparison.

The applied prior art reference relates to a computer system with a tamper detecting function 3 of detecting tampering of files upon boot-up of the computer system (see Abstract, FIG. 1 of the applied prior art reference). The Office Action takes the position that the claimed "hardware secure module having a tamper resistant module structure and storing information related to secure software" is taught in paragraph [0037] of the cited reference. Applicant respectfully disagrees. The indicated paragraph merely explains the auxiliary storage device 4 in Fig. 1. It does not anticipate "a ***hardware secure module having a tamper resistant module structure*** and storing information related to secure software".

Further, the applied prior art reference describes in paragraphs [0035] to [0036] providing a ***boot program 2*** stored in ROM 1 of controller 100 in Fig. 1 with tamper detecting function 3, and, in paragraph [0038] that tamper detecting function 3 comprises tamper detecting unit 33. The Office Action suggests that this tamper detecting unit 33 corresponds to the claimed "falsification checking unit." Applicant respectfully disagrees. The tamper detecting unit 33 disclosed in the applied prior art reference is a part of a tamper detecting function 3 of boot

program 2, which is software, and not "a falsification checking unit that is ***loaded on the hardware secure module***".

Furthermore, according to paragraphs [0037]-[0041] of the applied prior art reference, the tamper detecting unit 33 compares first stored information 41 (e.g., a digital signature) read out from auxiliary storage device 4 with second stored information 34 (e.g., a key for signature check) of the boot program 2. Therefore, tamper detecting unit 33 of the applied prior art reference does not anticipate and it is not inherent a "falsification checking unit", which "***reads the secure software*** from the memory by direct access without using an operating system, ***compares the secure software with the information in the hardware secure module, and checks whether the secure software is falsified based on a result of the comparison***" as recited in claim 1.

Therefore, the applied prior art references fails to anticipate independent claim 1. Claims 2-4, and 6-19 depending directly or indirectly from independent claim 1, patentably distinguish over the applied prior art at least by inheriting patentable features from independent claim 1.

Independent claim 20 patentably distinguishes over the prior art at least by reciting:

- reading secure software stored in a memory **using direct access method without using an operating system, by a hardware secure module having a tamper resistant module structure** which stores information related to the secure software;
- checking falsification by **a falsification checking unit that is loaded on the hardware secure module, by comparing the secure software with the information**, and determining whether the secure software is falsified based on a result of the comparison. (Emphasis added for the missing features in view of the above-discussion.)

Independent claim 21 and claims 22-24 and 26-39 depending directl;y or indirectly from independent claim 21 patentably distinguish over the applied prior art at least due to the following features recited in claim 21:

- a reading unit that reads a secure software **from a memory mounted to the information reproducing apparatus by direct access without using an operating system**; and
- a falsification checking unit that **compares the secure software with information related to the secure software stored in the hardware secure module, and checks a**

falsification of the secure software based on a result of the comparison, wherein if the result of the comparison shows that the secure software is not falsified the secure software is executed by the information reproducing apparatus. (Emphasis added for the missing features in view of the above-discussion.)

Independent claim 40 patentably distinguishes over the applied prior art at least by reciting:

- reading secure software stored in a memory **using a direct access method and without using an operating system, by the hardware secure module having a tamper resistant module structure storing information related to the secure software**;
- checking falsification **by comparing the secure software with the first information, and determining a falsification of the secure software based on a result of the comparison**. (Emphasis added for the missing features in view of the above-discussion.)

Independent claim 41 patentably distinguishes over the applied prior art at least by reciting:

- executing secure software that is stored in a memory accessible to an information reproducing apparatus **using a direct access method, if comparison of the secure software with information related to the secure software stored in a hardware secure module having a tamper resistant module structure inaccessible from outside, indicates that the secure software is not falsified**. (Emphasis added for the missing features in view of the above-discussion.)

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

/Luminita Todor/

Date: March 4, 2010 By: _____

Luminita A. Todor
Registration No. 57,639

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501